Technical Cybersecurity

NMAP Details

Other Info

NMAP COLLECTS OTHER DETAILS

- -O and -sV options
- -O option uses second generation techniques
  - First generation techniques aren’t available in new versions of NMAP
- -sV will attempt to version the OS and Services
- -A executes OS fingerprinting, version scans, script scans (more later on this) and traceroute

v. scanme.nmap.org

OS SCAN

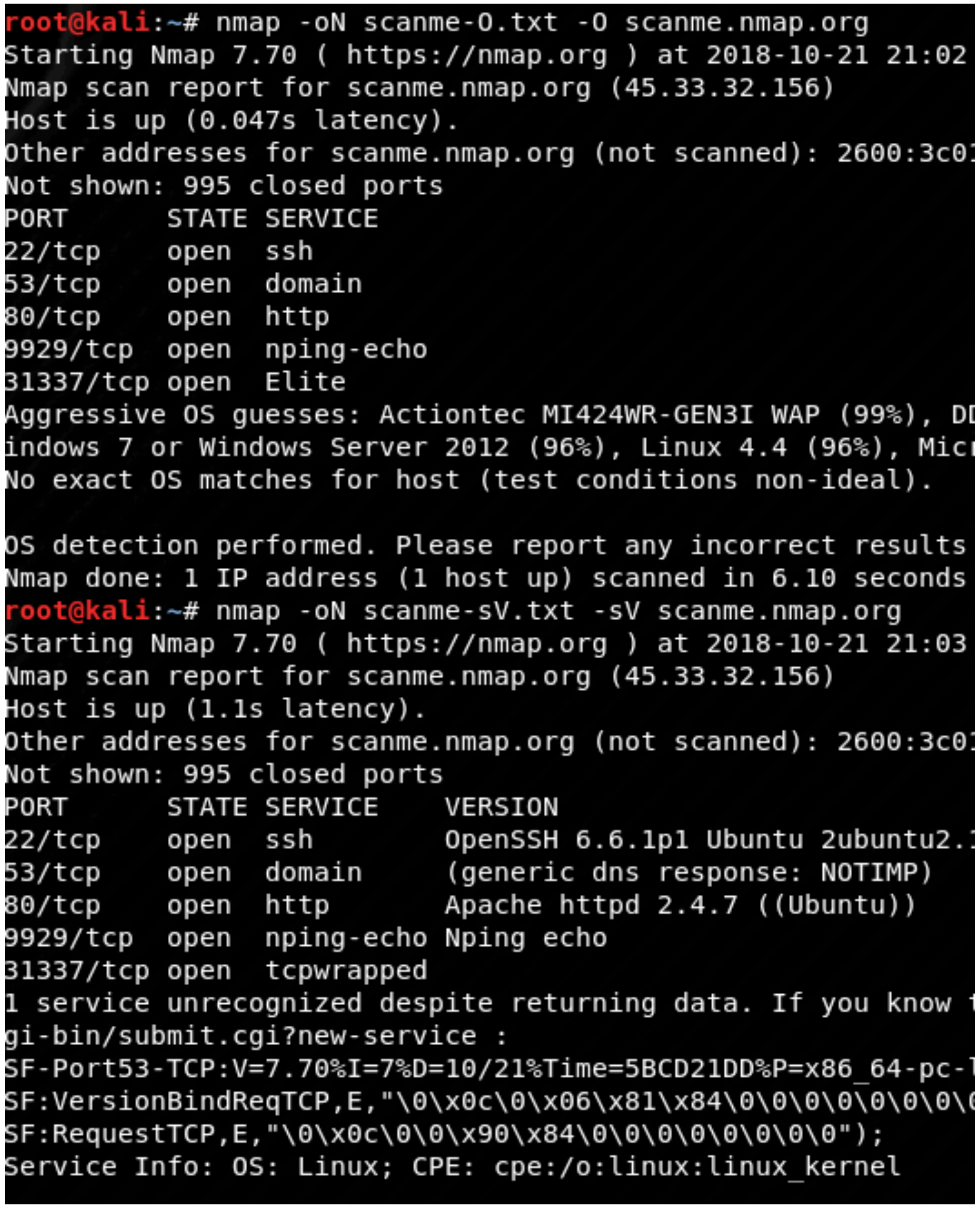
- nmap -oN scanme-O.txt -O scanme.nmap.org

VERSION DETAILS

- nmap -oN scanme-sV.txt -sV scanme.nmap.org

GET IT ALL!

- nmap -oN scanme-A.txt -A scanme.nmap.org



```
root@kali:~# nmap -oN scanme-O.txt -O scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-21 21:02
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.047s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c0
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite
Aggressive OS guesses: Actiontec MI424WR-GEN3I WAP (99%), DD
indows 7 or Windows Server 2012 (96%), Linux 4.4 (96%), Mic
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results
Nmap done: 1 IP address (1 host up) scanned in 6.10 seconds
root@kali:~# nmap -oN scanme-sV.txt -sV scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-21 21:03
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (1.1s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c0
Not shown: 995 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.
53/tcp    open  domain     (generic dns response: NOTIMP)
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
1 service unrecognized despite returning data. If you know
gi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.70%I=7%D=10/21%Time=5BCD21DD%P=x86_64-pc-
SF:VersionBindReqTCP,E,"\0\x0c\0\x06\x81\x84\0\0\0\0\0\0\0\
SF:RequestTCP,E,"\0\x0c\0\0\x90\x84\0\0\0\0\0\0\0\0");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

NMAP Scripting

LUA SCRIPTING

- Embedded scripting engine
- Commonly used in games
- check out: https://www.lua.org

USING THEM

- nmap -sC …
- nmap —script={all|category|dir|script} …
- —script-trace, —script-help, —script-args {args}

Try a few

DEFAULT SCRIPTS

- nmap -sC scanme.nmap.org

VULNERABILITY SCRIPTS

- nmap --script=vuln scanme.nmap.org

VERSION SCRIPTS

- nmap --script=version scanme.nmap.org
- …sometimes the stock functions are better!

What have we learned?

LIKELY UBUNTU

- Our OS checker was ambiguous
- Versioning of services seemed to indicate an Ubuntu install

WHAT ELSE?

- Some known vulnerabilities exist
- The system uses tcpwrappers to protect some ports
- The HTTP server is Apache 2.4.7
  - …hmmm, kinda old!
- OpenSSH 6.6.1p1
  - Perhaps vulnerable to CVE-2016-0777 and CVE-2016-0778?

What else might it be vulnerable to?